

REMARKS

Claims 1-6 are pending in the application and stand rejected.

Rejection under 35 U.S.C §103

Claims 1, 2 and 6 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 6,009,177 to Sudia in view of U.S. Pat. No. 6,430,561 to Austel and evidenced by ISO/IEC-15408. In particular, the Examiner finds that, with respect to claims 1 and 6, Sudia teaches all claimed elements with the exception of a controller for assigning a trust level as recited in the claims. However, the Examiner finds that Austel teaches a controller for assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric. In support of this assertion, the Examiner refers us back to Sudia and cites to column 13, lines 33-36 and Fig. 8. The Examiner thus opines that it would have been obvious to the person of ordinary skill to combine the teachings of Austel with the system of Sudia because Austel teaches the prevention of tampering and unauthorized modification to files (this time citing to Austel at column 6, lines 39-40).

Applicants have reviewed the two references with care, paying particular attention to the passages and figures cited to by the Examiner, and are compelled to disagree with the Examiner's understanding of these references. Sudia generally relates to a chip device that acts as a trusted device for the user and that contains a number of secrets, some of which may be externally disclosed and some not (see, e.g., col. 16, l. 9 to col. 17, l. 27). None of these secrets are described as being a measurement relating to the integrity of the trusted device or of a computing entity to which it relates, and therefore none of these secrets are, or are capable of performing the function of, an integrity metric as claimed. As Sudia clearly shows in Figure 24 and in the related text at 43:54 - 45:57, the trusted device of Sudia interacts with a trusted third party to receive permission to conduct certain classes of transactions (col. 43, l.54 – col. 45, l. 57) such that the trusted third party can obtain “some information to identify the user and the nature of the registration request” and “other information and assurances from either the user or from other parties to verify the user's identity, affiliation, creditworthiness, etc.” (col. 44, ll. 14-29) to determine whether this permission can be granted. If permission can be granted, the

trusted third party provides an appropriate certificate, possibly accompanied by downloadable firmware and keys (col. 44, ll. 30-55, also cited to by the Examiner). Information verifying the user's identity, affiliation, creditworthiness, etc. is certainly not, nor an equivalent to, an integrity metric having values for a plurality of characteristics associated with a computer entity. The disclosure at column 16, lines 5-67 cited to by the Examiner contains merely a recitation of information that may be permanently embedded by a manufacturer into a protected memory area of a device. This too cannot possibly be read as corresponding to an integrity metric having values for a plurality of characteristics associated with a computer entity as claimed and further described in the specification of the application.

Applicants respectfully remind the Examiner of the requirements posited by MPEP 2143.03 that "[t]o establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). All words in a claim must be considered in judging the patentability of that claim against the prior art. *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970)." (emphasis added) As fully set forth above, the Examiner has not made and indeed cannot make a *prima facie* showing that Sudia teaches the use of an integrity metric and, should the Examiner desire to insist that Sudia discloses the use of an integrity metric as recited in the claims, Applicants respectfully request that the Examiner to cite the precise language where Sudia explicitly discloses the use of an integrity metric as claimed herein in conjunction with the present disclosure. In light of the above, Applicants submit that claims 1 and 6 are in fact nonobvious and allowable and respectfully requests the Examiner to reconsider and pass these claims to issue.

In the interest of fully responding to the Examiner's Action, Applicants further address Austel. Austel is directed to a method for implementing a security policy for controlling access by programs to protected files. The method of Austel assigns access classes to files and to accessing programs, and allows files to be accessed and operated on only in accordance with an appropriate set of rules. Each access class includes an integrity access class and a secrecy access class, each comprising rules for read, write and execute functions. One embodiment is described as assigning the integrity access class "based on the results of an independent external evaluation process" such as ITSEC and EAL (col. 10, ll. 44-58). There is absolutely no disclosure in Austel

of anything akin to calculating an integrity metric as recited in the claims. The Examiner appears to assume that, because Austel terms one of the classes an "integrity access class," it is the same as the integrity metric of the present claims. This is simply not supported by the plain language of Austel and Applicants once again respectfully invite the Examiner to cite the precise language where Austel explicitly discloses the use of an integrity metric as claimed herein in conjunction with the present disclosure, or else to withdraw this rejection.

Applicants further note that the motivation to one skilled in the art to combine the Austel and Sudia references is also completely lacking, despite the Examiner's assertion to the contrary. The Examiner explicitly states that the motivation perceived in Austel is that Austel teaches the prevention of tampering and unauthorized modification to files. As also noted by the Examiner, part of the process of Austel is the allocation of an access class to an accessing program to access files. This has nothing whatsoever to do with one computing entity determining trust to be placed in another computing entity. Austel contains absolutely no teaching at all concerning the determination of trust in one computer entity by another computer entity, and actually teaches away from applying his teachings to such a method for determination of trust in one computer entity by another computer entity by teaching that the assignment of an access class to an accessing program is a task carried out by a system administrator (col. 9, ll. 33-35). Thus, Austel does not on fact provide motivation to one skilled in the art to apply his teachings to the method of Sudia; nonetheless, as set forth above, even if such a combination of references were attempted, the result would not anticipate the present claims.

Further in the interest of completeness, Applicants note that section 4.1.1 of ISO/IEC-15408 Part I is also not in the least bit anticipatory of the present invention. The paragraph cited by the Examiner notes that owners of assets need to be confident that countermeasures are adequate to counter threats before assets are exposed to such threats. Such countermeasures should therefore be "evaluated", the result comprising an "assurance rating" to be used by the asset owner to determine whether to accept the risk of exposure to threats. This section is wholly lacking in teaching as to how to achieve this desirable result. It certainly does not even hint that integrity metrics could or should play any role in achieving this result. The present invention, in embodiments, may in fact be used to achieve the desirable result outlined here – which, of course, is an indication that the invention is useful, not that it is obvious.

In view of the above, Applicants respectfully request the Examiner to withdraw the rejection of claims 1, 2 and 6 and pass these claims to issue.

Claims 3-4 depend from claim 1. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion of claim 1, Applicants submit that claims 3-4 are also nonobvious and allowable.

Applicants have amended claims 1 and 6 to conform more closely to current U.S. practice. These amendments are made solely for the purpose of making the claims easier to read and Applicants expressly note that therefore these amendments are not made for purposes related to patentability, because the amendments do not alter the scope of the claim.

Applicants further present new claims 7-61, together with an authorization to charge the excess claims fee to our deposit account. These claims are all directed to originally disclosed subject matter and introduce no new matter into the application. All of these claims are novel over the cited art for the same reasons discussed above, and Applicants respectfully urge the Examiner to pass these claims to issue along with claims 1-6.

In view of the above, Applicants submit that the application is now in condition for allowance and respectfully urge the Examiner to pass this case to issue.

A Notice of Change of Correspondence Address is filed concurrently herewith. Kindly note the new Attorney Docket Number for this case.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Non-Fee Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

December 9, 2004

(Date of Transmission)

Mia Kim

(Name of Person Transmitting)

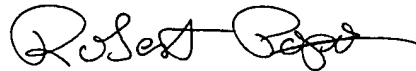


(Signature)

12/9/04

(Date)

Respectfully submitted,



Robert Popa

Attorney for Applicants

Reg. No. 43,010

LADAS & PARRY

5670 Wilshire Boulevard, Suite 2100

Los Angeles, California 90036

(323) 934-2300 voice

(323) 934-0202 facsimile

rpopa@ladasparry.com